

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

_____)	
In the Matter of)	
)	DOCKET NO. C-4400
CBR SYSTEMS, INC.)	
)	DECISION AND ORDER
)	
_____)	

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment filed by an interested person, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent Cbr Systems, Inc. is a California corporation with its principal office or place of business at 1200 Bayhill Drive, Suite 301, San Bruno, California 94066.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Cbr Systems, Inc., and its successors and assigns.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) a bank account, debit card, or credit card account number; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number; (i) clinical laboratory testing information, including test results; or (j) the fact and circumstances of a child’s adoption, such as whether the birth mother was a surrogate. For the purpose of this provision, a “consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which it uses, maintains, and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. This section may be satisfied through the review and maintenance of an existing program so long as that program fulfills the requirements set forth herein. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of the information security program in light of the results of the testing and monitoring required by subpart C, any material changes to any operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. certify that the security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Cbr Systems, Inc.*, FTC File No.1123120. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment;
- B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this order, including but not limited to:
 - 1. all advertisements and promotional materials containing any representations covered by this order, with all materials used or relied upon in making or disseminating the representation; and
 - 2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver copies of the order as directed below:

- A. Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondent shall secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Cbr Systems, Inc.*, FTC File No.1123120. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on April 29, 2033, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL

ISSUED: April 29, 2013